SENADO FEDERAL

REQUERIMENTO Nº DE

Requer que sejam prestadas, pelo Senhor Ministro de Estado da Justiça e Segurança Pública, Wellington César Lima e Silva, informações acerca de providências adotadas diante do incidente cibernético ocorrido na madrugada do dia 20 de junho de 2026, com envio indevido de mensagem para milhares de pessoas no País, classificada como "Alerta Extremo" pelo sistema Defesa Civil Alerta, acompanhada do sinal sonoro característico desse nível de emergência e contendo a palavra "misantropi4".

Senhor Presidente,

Requeiro, nos termos do art. 50, § 2º, da Constituição Federal e dos arts. 216 e 217 do Regimento Interno do Senado Federal, que sejam prestadas, pelo Senhor Ministro de Estado da Justiça e Segurança Pública, Wellington César Lima e Silva, informações acerca de providências adotadas diante do incidente cibernético ocorrido na madrugada do dia 20 de junho de 2026, com envio indevido de mensagem para milhares de pessoas no País, classificada como "Alerta Extremo" pelo sistema Defesa Civil Alerta, acompanhada do sinal sonoro característico desse nível de emergência e contendo a palavra "misantropi4".

Nesses termos, requisita-se:

I – DA INVESTIGAÇÃO CRIMINAL

1. Confirme se foi instaurado inquérito policial ou outro procedimento investigatório para apuração dos fatos, informando:

a) a data de instauração;

b) a unidade responsável;

c) o objeto da investigação; e

d) o estágio atual das apurações.

2. Informe qual a linha investigativa atualmente adotada pela Polícia Federal, esclarecendo se há indícios de:

a) ataque cibernético externo;

b) comprometimento de credenciais legítimas;

c) exploração de vulnerabilidade tecnológica;

d) falha operacional;

e) ação interna; ou

f) outra hipótese em investigação.

3. Informe se há indícios da participação de organização criminosa, grupo especializado em crimes cibernéticos, agentes estrangeiros ou atuação coordenada destinada ao comprometimento de infraestrutura tecnológica governamental e/ou se a Polícia Federal realizou análise técnica e investigativa acerca do conteúdo da mensagem indevidamente difundida, especialmente da utilização da palavra "misantropia", indicando se foram identificados elementos que possam contribuir para a identificação da autoria, da motivação, do perfil dos responsáveis, da eventual vinculação a grupos organizados, comunidades virtuais voltadas à prática de crimes cibernéticos, extremismo violento ou disseminação de discursos de ódio, bem como eventual propósito de provocar temor coletivo, descrédito nas instituições públicas ou perturbação da ordem social.

4. Informe se houve solicitação de cooperação técnica, policial ou jurídica internacional, indicando os países, organismos internacionais ou instituições eventualmente acionados.

5. Informe se foram preservadas todas as evidências digitais necessárias à perícia forense, especialmente:

a) registros de auditoria (logs);

b) trilhas de auditoria;

c) registros de autenticação;

d) registros de acesso privilegiado;

e) imagens dos ambientes computacionais; e

f) demais elementos técnicos necessários à identificação da origem do incidente.

6. Informe se foram identificados indícios de comprometimento de outros sistemas governamentais, da reutilização da mesma vulnerabilidade em outras plataformas da Administração Pública Federal ou da existência de campanhas coordenadas contra infraestruturas críticas nacionais ou se foram identificados indícios de movimentação semelhante contra outras infraestruturas críticas da União, ainda que não tenham sido efetivamente comprometidas.

II – DA COORDENAÇÃO DA RESPOSTA GOVERNAMENTAL

7. Informe quais órgãos e entidades federais participam da resposta ao incidente, especificando as respectivas competências e atribuições.

8. Informe se foi acionado protocolo nacional de resposta a incidentes cibernéticos, indicando:

a) a data do acionamento;

b) os órgãos envolvidos;

c) as medidas imediatamente adotadas; e

d) os procedimentos atualmente em execução.

9. Informe se o incidente foi comunicado ao Centro Integrado de Segurança Cibernética do Governo Federal, ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) ou a outro órgão especializado em resposta a incidentes, especificando:

a) a data da comunicação;

b) os órgãos envolvidos;

c) as recomendações técnicas emitidas;

d) as providências adotadas em decorrência dessas recomendações; e

e) se permanecem em acompanhamento do caso.

10. Informe se o incidente foi classificado como incidente relevante envolvendo infraestrutura crítica nacional ou outra categoria equivalente de risco, indicando os fundamentos técnicos adotados.

11. Informe se foram expedidas recomendações, determinações ou alertas aos demais órgãos e entidades da Administração Pública Federal visando prevenir episódios semelhantes, encaminhando cópia das orientações de caráter público.

12. Informe se, antes do incidente ocorrido em 20 de junho de 2026, esse Ministério, a Polícia Federal ou quaisquer órgãos a ele vinculados receberam comunicações, auditorias, alertas técnicos, relatórios de vulnerabilidade, notificações, recomendações ou quaisquer outras informações relativas a riscos envolvendo o sistema Defesa Civil Alerta, a infraestrutura tecnológica utilizada para emissão de alertas públicos ou sistemas governamentais correlatos.

Em caso positivo, informar:

a) a origem do alerta;

b) a data de seu recebimento;

c) a classificação do risco apontado;

d) as providências adotadas;

e) eventual comunicação aos demais órgãos competentes; e

f) os motivos pelos quais o risco persistiu, caso isso tenha ocorrido.

13. Informe se o Ministério da Justiça e Segurança Pública pretende revisar protocolos nacionais de prevenção, investigação, resposta e recuperação de incidentes cibernéticos em razão dos fatos ora apurados, indicando as principais medidas que se encontram em estudo.

III – DA PROTEÇÃO DE DADOS PESSOAIS E DA ATUAÇÃO DA ANPD

14. Informe se a Autoridade Nacional de Proteção de Dados – ANPD foi formalmente comunicada acerca do incidente, indicando:

a) a data da comunicação;

b) o órgão responsável pela comunicação; e

c) a finalidade da comunicação realizada.

15. Informe se houve articulação institucional entre este Ministério e a ANPD para avaliação dos possíveis reflexos do episódio sob a perspectiva da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), encaminhando, quando possível, as respectivas manifestações técnicas de caráter público.

16. Informe se, até o presente momento, foram identificados indícios de comprometimento de dados pessoais, credenciais, registros eletrônicos, bases cadastrais, informações de autenticação ou quaisquer outros elementos sujeitos à proteção da LGPD.

17. Caso inexistam, até o momento, indícios de comprometimento de dados pessoais, informe quais elementos técnicos fundamentam essa conclusão preliminar e se novas análises periciais permanecem em andamento.

18. Informe se a ANPD instaurou procedimento administrativo de acompanhamento, fiscalização ou orientação relacionado ao incidente e, em caso positivo, qual o estágio atual desse procedimento.

19. Informe se houve avaliação acerca da necessidade de comunicação formal do incidente à ANPD, indicando os fundamentos técnicos e jurídicos adotados para a decisão.

20. Informe se foram expedidas recomendações técnicas relativas:

a) à segurança da informação;

b) à governança de dados pessoais;

c) à gestão de riscos cibernéticos;

d) ao fortalecimento dos controles internos; e

e) às medidas preventivas aplicáveis aos órgãos responsáveis pelo sistema Defesa Civil Alerta.

IV – DA COMUNICAÇÃO COM A POPULAÇÃO

21. Informe quais medidas de comunicação institucional foram adotadas para esclarecer a população acerca do ocorrido e para preservar a credibilidade do sistema Defesa Civil Alerta.

22. Informe se foram identificados registros de golpes, fraudes, campanhas de desinformação, tentativas de engenharia social ou outras práticas ilícitas relacionadas à ampla divulgação do incidente.

23. Informe se foram expedidas orientações específicas aos cidadãos para prevenção de eventuais golpes ou fraudes decorrentes do episódio, encaminhando cópia das comunicações públicas produzidas.

24. Informe se houve monitoramento de redes sociais, aplicativos de mensagens ou outros ambientes digitais para identificação de campanhas coordenadas de desinformação relacionadas ao incidente, indicando, quando possível, os resultados obtidos.

V – DA PREVENÇÃO E DO APERFEIÇOAMENTO INSTITUCIONAL

25. Informe quais medidas estruturantes esse Ministério pretende adotar, isoladamente ou em articulação com outros órgãos da Administração Pública Federal, para fortalecer a prevenção, a detecção e a resposta a incidentes cibernéticos envolvendo infraestruturas críticas nacionais.

26. Informe se o episódio ensejará revisão dos protocolos de integração entre os órgãos responsáveis pela segurança pública, pela segurança cibernética, pela proteção de dados pessoais e pela defesa civil, indicando as principais medidas em estudo.

VI – DA TRANSPARÊNCIA E DA PRESTAÇÃO DE CONTAS

27. Informe se será elaborado relatório conclusivo da investigação criminal ou relatório técnico consolidado sobre o incidente, indicando, quando possível, o prazo estimado para sua conclusão.

28. Informe se referido relatório, ressalvadas as informações protegidas por sigilo legal, será encaminhado ao Congresso Nacional ou disponibilizado ao público.

29. Encaminhe cópia dos atos administrativos públicos relacionados à instauração dos procedimentos investigatórios, das notas técnicas, pareceres, orientações expedidas aos órgãos federais e demais documentos públicos

produzidos em decorrência do incidente, ressalvadas apenas as informações protegidas por sigilo legal.

30. Encaminhe cópia dos relatórios técnicos, pareceres, notas técnicas, auditorias, recomendações, comunicações internas de caráter ostensivo, planos de ação e demais documentos públicos produzidos em decorrência do incidente, indicando expressamente, quando houver restrição de acesso a qualquer documento solicitado, o respectivo fundamento jurídico da negativa, com especificação da norma legal aplicável.

JUSTIFICAÇÃO

Segundo divulgado por veículos de comunicação e por inúmeras pessoas, na madrugada do dia 20 de junho de 2026, milhões de brasileiros foram surpreendidos pelo recebimento, em seus aparelhos celulares, de mensagem classificada como "Alerta Extremo", acompanhada do sinal sonoro característico reservado às comunicações de risco iminente à vida, emitida por meio do sistema Defesa Civil Alerta. A mensagem, entretanto, não correspondia a qualquer desastre natural, emergência ou situação concreta que justificasse o acionamento da ferramenta, limitando-se à divulgação da palavra "misantropia", fato que provocou insegurança na população e ampla repercussão nacional.

Em razão da gravidade do ocorrido, o Governo Federal informou a suspensão preventiva da plataforma, comunicou a adoção de medidas emergenciais para contenção do incidente e anunciou a instauração de procedimentos destinados à apuração de possível ataque cibernético, com atuação da Polícia Federal e de outros órgãos competentes.

Os fatos possuem elevada relevância institucional por envolverem sistema concebido para proteção da população em situações de emergência, utilizado para alertar sobre enchentes, deslizamentos, rompimentos de barragens,

incêndios florestais, tempestades severas e outros eventos capazes de colocar em risco a vida e a integridade física de milhares de brasileiros.

A credibilidade desse instrumento constitui elemento indispensável para sua efetividade. A emissão de alertas extremos pressupõe que a população reconheça a autenticidade das mensagens e adote imediatamente as medidas de autoproteção indicadas pelas autoridades competentes. Qualquer comprometimento dessa confiança possui potencial para reduzir a eficácia dos futuros alertas legítimos e comprometer a resposta da sociedade diante de situações reais de desastre.

Paralelamente aos impactos sobre a política nacional de proteção e defesa civil, o episódio desperta preocupação quanto à proteção das infraestruturas tecnológicas estratégicas do Estado brasileiro e à capacidade institucional de prevenção, detecção e resposta a incidentes cibernéticos que possam atingir sistemas governamentais essenciais.

A própria mensagem indevidamente difundida também constitui elemento que merece especial atenção investigativa. A utilização da palavra "misantropia", termo associado à aversão ou desprezo pela humanidade, revela conteúdo incomum para comunicações oficiais de emergência e pode representar importante elemento para a compreensão da motivação, da intencionalidade e do contexto em que o incidente foi praticado. Sem antecipar conclusões quanto à autoria ou ao enquadramento jurídico dos fatos, mostra-se relevante esclarecer se a escolha dessa expressão possui eventual significado investigativo, se guarda relação com grupos ou comunidades virtuais voltadas à prática de crimes cibernéticos, extremismo violento ou disseminação de discursos de ódio, ou se constitui mera tentativa de provocar temor coletivo, descrédito nas instituições públicas ou perturbação da ordem social. Trata-se de aspecto diretamente relacionado às atribuições investigativas da Polícia Federal e que reforça o interesse público na adequada elucidação dos fatos.

Sob essa perspectiva, a atuação do Ministério da Justiça e Segurança Pública assume especial relevância. Compete à Pasta, por intermédio da Polícia Federal e dos demais órgãos integrantes de sua estrutura, promover a investigação de eventuais ilícitos penais praticados contra bens, serviços e interesses da União, bem como coordenar ações relacionadas ao enfrentamento da criminalidade cibernética, à preservação das evidências digitais e à articulação institucional necessária à adequada resposta estatal.

A atuação tempestiva, coordenada e tecnicamente fundamentada dos órgãos de persecução penal mostra-se essencial não apenas para identificação e responsabilização dos autores, mas também para esclarecer a dinâmica do incidente, avaliar sua extensão, verificar eventual comprometimento de outras infraestruturas críticas e subsidiar o aperfeiçoamento dos protocolos nacionais de segurança cibernética.

Também se revela imprescindível esclarecer se, anteriormente ao incidente, órgãos integrantes do Ministério da Justiça e Segurança Pública, da Polícia Federal ou de sua estrutura de segurança cibernética receberam comunicações, relatórios técnicos, auditorias, notificações, recomendações ou alertas acerca de vulnerabilidades relacionadas ao sistema Defesa Civil Alerta ou a outras infraestruturas tecnológicas correlatas. A identificação de eventuais alertas prévios, bem como das providências adotadas em resposta a essas comunicações, constitui elemento indispensável para aferição da efetividade da gestão de riscos, da governança da segurança da informação e dos mecanismos preventivos existentes no âmbito da Administração Pública Federal.

Outro aspecto igualmente relevante refere-se à eventual repercussão do incidente sob a ótica da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Embora, até o presente momento, não haja confirmação oficial acerca de comprometimento de dados pessoais, mostra-se imprescindível esclarecer se essa hipótese foi tecnicamente analisada, se houve articulação institucional com a Autoridade Nacional de Proteção de Dados – ANPD

e quais conclusões preliminares foram alcançadas pelos órgãos competentes. A presente iniciativa não parte da premissa de que tenha ocorrido incidente envolvendo dados pessoais, mas busca conferir transparência quanto às avaliações técnicas realizadas pelo Poder Executivo e às providências eventualmente adotadas para resguardar a segurança da informação e a proteção de dados.

O presente Requerimento busca, ainda, compreender como se deu a coordenação entre os diversos órgãos federais responsáveis pela resposta ao incidente, incluindo os centros especializados em segurança cibernética, a Polícia Federal, a Autoridade Nacional de Proteção de Dados e os demais órgãos envolvidos na investigação e na contenção dos riscos. A adequada integração institucional constitui requisito essencial para o fortalecimento da resiliência das infraestruturas críticas nacionais e para o aperfeiçoamento permanente da capacidade estatal de resposta a eventos dessa natureza.

Cumpre destacar que compete ao Congresso Nacional exercer, nos termos do art. 49, inciso X, da Constituição Federal, o controle e a fiscalização dos atos do Poder Executivo. De igual modo, o art. 50, § 2º, da Constituição assegura às Casas do Congresso Nacional a prerrogativa de requisitar informações aos Ministros de Estado acerca de assuntos inerentes às respectivas atribuições, permitindo ao Parlamento acompanhar a implementação das políticas públicas e avaliar a eficiência da atuação administrativa.

As informações ora solicitadas permitirão ao Senado Federal exercer adequadamente sua função constitucional de fiscalização, contribuindo para o fortalecimento da segurança cibernética da Administração Pública Federal, para o aperfeiçoamento da governança das infraestruturas tecnológicas estratégicas, para a evolução dos mecanismos nacionais de prevenção e resposta a incidentes cibernéticos e para a preservação da confiança da população nos sistemas oficiais destinados à proteção da vida.

Diante da elevada relevância institucional dos fatos e do inequívoco interesse público envolvido, impõe-se o encaminhamento do presente Requerimento de Informações.

Sala das Sessões, 22 de junho de 2026.

Senadora Damares Alves